FIG. 1

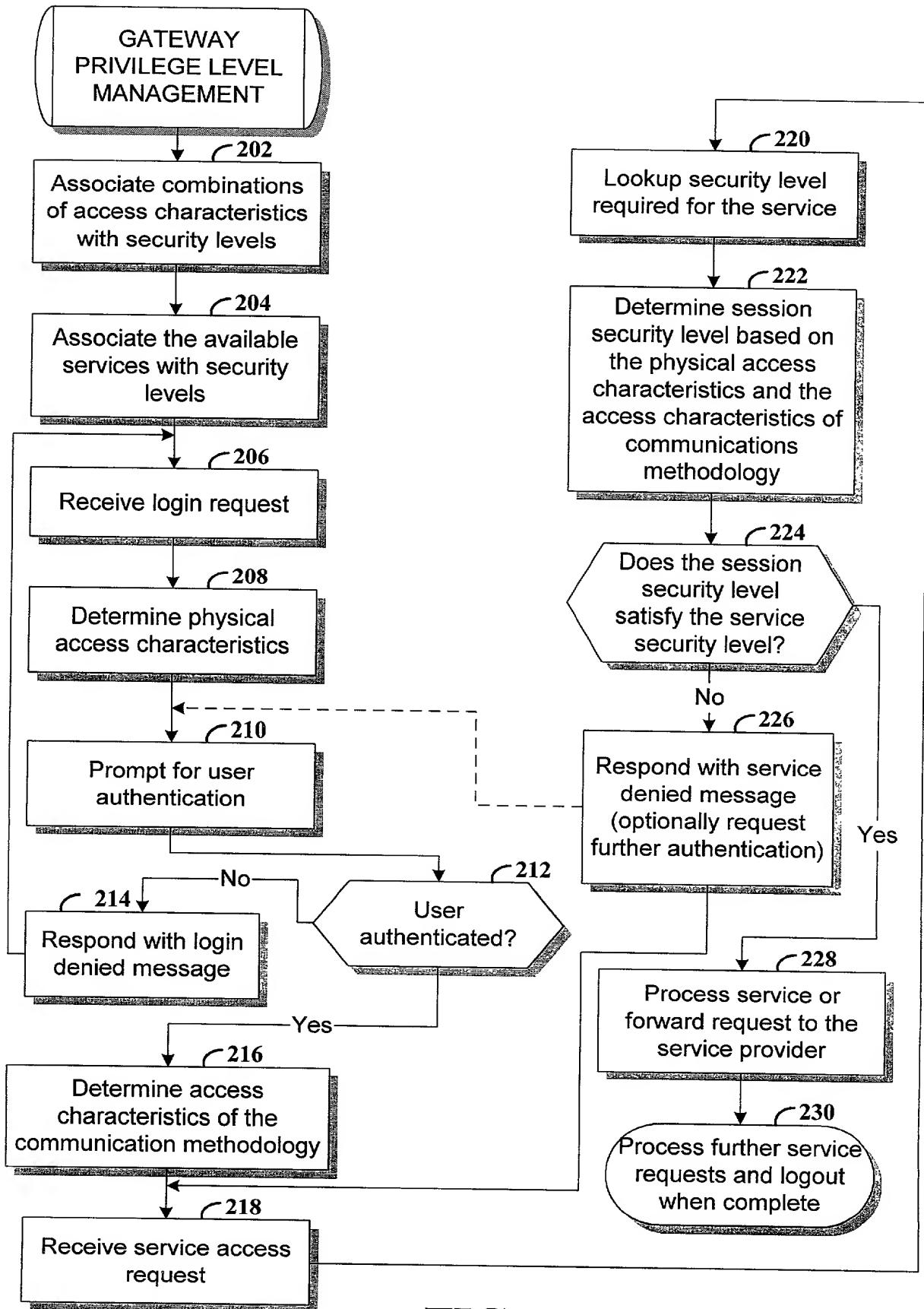| ACCESS CHARACTERISTICS	SECURITY LEVEL
password only	2
MSISDN number (no login required)	1
weak encryption and password only	3
weak encryption and certificate only	2
weak encryption and password plus device identifier (MSISDN or certificate)	4
strong encryption and password only	6
strong encryption, password, and device identifier	8
strong encryption, password, and smart card	8

FIG. 3

GATEWAY
PRIVILEGE LEVEL
MANAGEMENT

202
Associate combinations
of access characteristics
with security levels

204
Associate the available
services with security
levels

206
Receive login request

208
Determine physical
access characteristics

210
Prompt for user
authentication

214
Respond with login
denied message

No

212
User
authenticated?

Yes

216
Determine access
characteristics of the
communication methodology

218
Receive service access
request

220
Lookup security level
required for the service

222
Determine session
security level based on
the physical access
characteristics and the
access characteristics of
communications
methodology

224
Does the session
security level
satisfy the service
security level?

No

226
Respond with service
denied message
(optionally request
further authentication)

Yes

228
Process service or
forward request to the
service provider

230
Process further service
requests and logout
when complete

FIG. 2

352

SERVICE	SECURITY LEVEL
general information	0
account history	2
set preferences	2
change user profile	2
perform payment transaction	6

FIG. 4A

354

SERVICE	SECURITY LEVEL
general information	1
account history	3
set preferences	3
change user profile	3
perform payment transaction	7

FIG. 4B

356

SERVICE	SECURITY LEVEL
general information	1
account history	3
set preferences	3
change user profile	3
perform payment transaction < $500	6
perform payment transaction >= $500	7

FIG. 4C

358

SERVICE	SECURITY LEVEL = STANDARD	SECURITY LEVEL = HIGH
general information	0	2
account history	2	6
set preferences	2	6
change user profile	2	6
perform payment transaction	6	8

FIG. 4D